BL(u)E CRAB: A User-Centric Framework for Identifying Suspicious Bluetooth Trackers

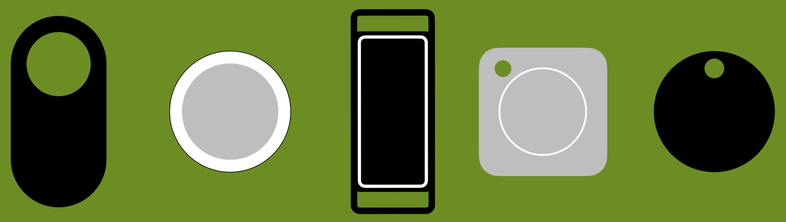
Dylan Conklin
Portland State University

Primal Pappachan
Portland State University

Roberto Yus
University of Maryland, Baltimore County

Motivation

Bluetooth Low Energy (BLE) trackers are devices that can be used to locate lost items, but they are commonly misused for stalking because of their convenience and small size. Such devices include AirTags, Tiles, SmartTags, PebbleBees and Chipolos.



Key Privacy Features

- Does not collecting user login data
- Independent from any web services
- Stores all data on-device
- Does not require location permissions
- Does not block functionality if location access is denied

Prior Work

BLE tracking alert approaches do not adequately alert users[1]. This is partially due to device incompatibilities and lack of manufacturer participation. AirGuard[2] addresses these problems, but have limitations because of the static thresholds used to evaluate risk.

BL(u)E CRAB introduces a metric-driven risk method based on dynamic thresholds derived from various risk factors.

References

[1] H. et al., "Please unstalk me: Understanding stalking with bluetooth trackers and democratizing anti-stalking protection," PoPETS Proceedings, 2024.

[2] H. et al., "Airguard - protecting android users from stalking attacks by apple find my devices," ser. WiSec '22, Association for Computing Machinery, 2022, ISBN: 9781450392167.

[3] B. et al., "Ble-doubt: Smartphone-based detection of malicious bluetooth trackers," in SafeThings 2022, IEEE.

Risk Factors

Time with User: Measures the duration of time a devices is near the user.

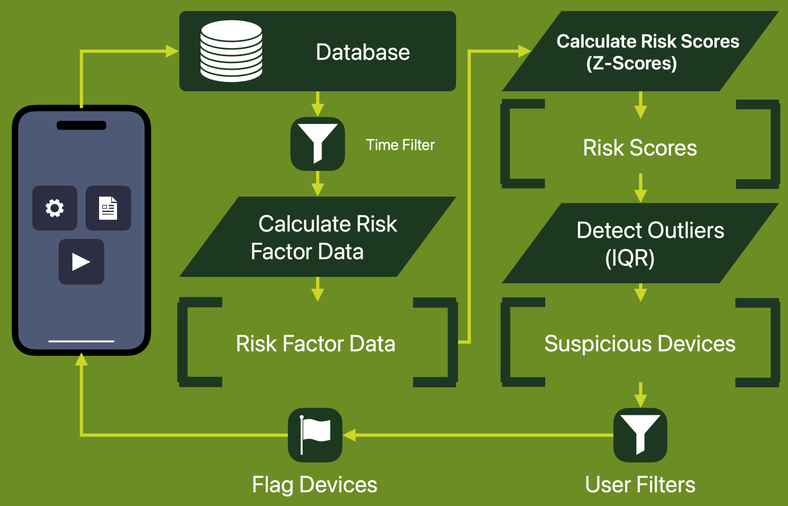
Incidence: Counts the number of "run-ins" the user has with a device.

Distance Travelled with User: Measures the distance a device has travelled with the user.

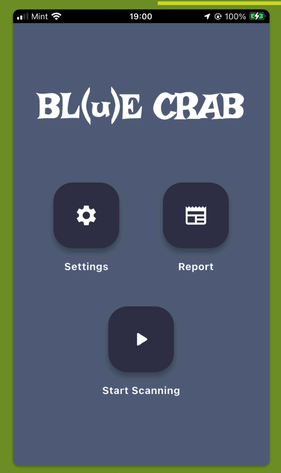
Area Count: Measures the amount of non-overlapping location clusters separated by a threshold distance.

Device Proximity: Measures the device's proximity via RSSI

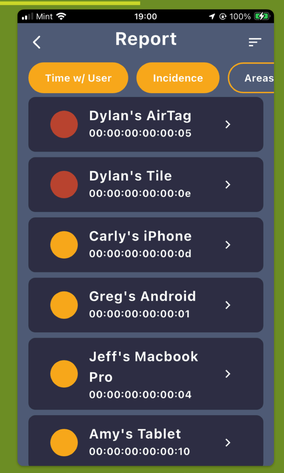
How BL(u)E CRAB Works



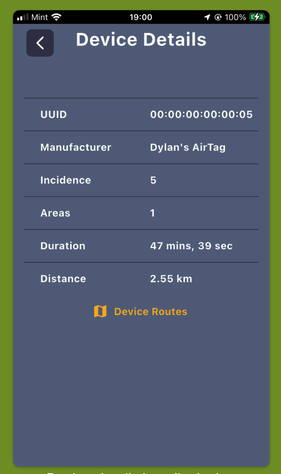
Screenshots



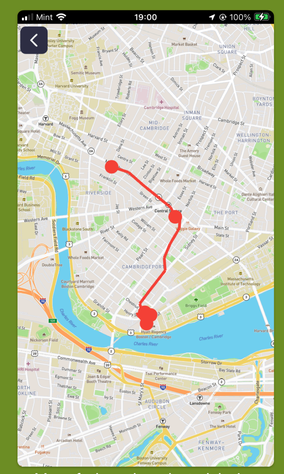
Scanner view with the scan button at the bottom



Report view with tiles for flagged devices



Device detail view displaying identifiers along with risk factors



Map of where the selected device traveled with the user

Future Work

- Improve outlier detection and add more risk factors
- Conduct empirical analysis
- Explain why a device is suspicious in a natural language

DIPr Lab

Portland State UNIVERSITY